UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/040,050	10/25/2001	Mahesh S. Maddury	50325-0598	1826

29989 7590 08/10/2005

HICKMAN PALERMO TRUONG & BECKER, LLP
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110

EXAMINER	
POWERS, WILLIAM S	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 08/10/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/040,050	MADDURY ET AL.	
	Examiner	Art Unit	
	William S. Powers	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 October 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 October 2001* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *10/25/2001*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-13 have been examined.

Drawings

2. The drawings are objected to:

a. Because figure 2 has no input register M as detailed in the specification (page 19, lines 3-5).

b. As failing to comply with 37 CFR 1.84(p)(5) because they include the following reference character(s) not mentioned in the description: figure 4, reference number 420.

Corrected drawing sheets in compliance with 37 CFR 1.121(d), or amendment to the specification to add the reference character(s) in the description in compliance with 37 CFR 1.121(b) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be

notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Objections

3. Claims 8-11 are objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form.

The claims modify the preamble of claim 5 and as such do not further limit the body of the claim.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claim 1 is rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential steps, such omission amounting to a gap between the steps. See MPEP § 2172.01. The omitted steps are: There is no step for the generation of the digital signature.

5. Claims 1-4, 6, 8, 9 and 12 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As to claims 1-4 and 12, the term "substantially equal" in claims 1-4 and 12 is a relative term which renders the claim indefinite. The term "substantially equal" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. It is not clear what "substantially equal" means in the context of the claims.

As to claim 6, Applicant describes the invention in the negative by pointing out what the invention is not.

As to claims 8 and 9, they contain the trademark/trade name RSA. Where a trademark or trade name is used in a claim as a limitation to identify or describe a particular material or product, the claim does not comply with the requirements of 35 U.S.C. 112, second paragraph. See *Ex parte Simpson*, 218 USPQ 1020 (Bd. App. 1982). The claim scope is uncertain since the trademark or trade name cannot be used properly to identify any particular material or product. A trademark or trade name is used to identify a source of goods, and not the goods themselves. Thus, a trademark or trade name does not identify or describe the goods associated with the trademark or trade name. In the present case, the trademark/trade name is used to identify/describe an encryption/decryption algorithm and, accordingly, the identification/description is indefinite.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

6. Claim 2 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

As to claim 2, the method steps manipulate abstract data. There is no "useful, concrete and tangible" result.

7. Claims 1-13 are rejected under 35 U.S.C. 101 because the claimed invention lacks patentable utility. The invention manipulates abstract data to an intermediate step, but does not actually produce the digital signature or any other tangible result.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

8. Claims 5, and 7-11 are rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent No. 4,759,063 to Chaum.

As to claim 5, Chaum teaches a modular multiplicative inverter (column 13, lines 33-35 and Figure 3).

As to claim 7, Chaum teaches that the multiplicative inverter operates in a sequential manner over a plurality of cycles (column 14, lines 6-55).

As to claims 8 and 9, Chaum teaches encoding and decoding using the RSA algorithm (column 4, line 58-column 5, line 29).

As to claims 10 and 11, Chaum teaches signing and verifying digital signatures (column 12, lines 32-68).

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 1-4, 12 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 4,759,063 to Chaum in view of "Applied Cryptography", 2nd edition, pages 248-249 by Schneier.

As to claims 1-4 and 12, Chaum teaches:

a. Receiving and storing integer data in a register (column 13, lines 33-37).

b. Computing a multiplicative inverse using modular arithmetic (column 13, lines 33-67).

c. Storing of the multiplicative inverse in a register (column 13, lines 33-61).

Chaum uses a modulus in modular arithmetic, but does not expressly mention that the modulus is a prime number.

Schneier teaches the exponent is 2 less than the modulus when using a prime modulus in a multiplicative inverse calculation (page 248-249). This is an accepted method for calculating the inverse with a prime modulus.

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to implement the invention of Chaum with the exponent that is 2 less than the prime modulus in multiplicative inverse calculations of Schneier. This is an accepted method for calculating the inverse with a prime modulus.

As to claim 13, Chaum teaches a modular exponentiator (column 11, lines 59-66).

Conclusion

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patent No. 4,405,829 to Rivest et al. discloses an exponentiation circuit, a message register, and encoding and decoding of messages.

U.S. Patent No. 4,891,781 to Omura discloses the use of chips and registers in modulo arithmetic.

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to William S. Powers, whose telephone number is (571) 272-8573. The examiner can normally be reached Monday-Thursday from 8 AM – 4:30 PM Eastern Time.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse, can be reached at (571) 272-3838.

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks
PO Box 1450
Alexandria, VA 22313-1450

Or faxed to:

(571) 273-8300

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at (886) 217-9197 (toll-free).

WSP

July 27, 2005

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100